

Generalization of Pigeon Hole Bound

Toni Ernvall

Department of Mathematics,
University of Turku

Abstract—H.-F. Lu, J. Lahtonen, R. Vehkalahti, and C. Hol-lanti introduced so called Pigeon Hole Bound for decay function of MIMO-MAC codes. Here we give a generalization for it.

I. DECAY FUNCTION

We consider here decay function of MIMO-MAC codes. Every user has some specific lattice $\mathbf{L}_j \subseteq \mathcal{M}_{n \times k}, j = 1, \dots, U$ with $k \geq Un$. We assume that each user's lattice is of full rank $r = 2kn$ so the lattice \mathbf{L}_j has an integral basis $B_{j,1}, \dots, B_{j,r}$. Now the code associated with j th user is a restriction of lattice \mathbf{L}_j such that

$$\mathbf{L}_j(N_j) = \left\{ \sum_{i=1}^r b_i B_{j,i} \mid b_i \in \mathbf{Z}, -N_j \leq b_i \leq N_j \right\}$$

where N_j is a given positive number.

Using these definitions the U -user mimo-mac code is $(\mathbf{L}_1(N_1), \mathbf{L}_2(N_2), \dots, \mathbf{L}_U(N_U))$.

For this we define

$$\mathfrak{D}(N_1, \dots, N_U) = \min_{X_j \in \mathbf{L}_j(N_j) \setminus \{0\}} \det(MM^\dagger)$$

where $M = M(X_1, \dots, X_U)$. For a special case $N_1 = \dots = N_U = N$ we write

$$\mathfrak{D}(N) = \mathfrak{D}(N_1 = N, \dots, N_U = N).$$

In the special case $k = Un$ we have

$$\mathfrak{D}(N_1, \dots, N_U) = D(N_1, \dots, N_U)^2$$

and especially

$$\mathfrak{D}(N) = D(N)^2.$$

II. AN UPPER BOUND USING PIGEON HOLE PRINCIPLE

So called Pigeon Hole Bound for decay function of MIMO-MAC codes was introduced in [1]. Here we give a generalization for it.

Lemma 2.1: Let $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{k-1} \in \mathbf{C}^n$, and $\mathbf{c}_i - \mathbf{e}_i \in L(\mathbf{c}_{i+1}, \mathbf{c}_{i+2}, \dots, \mathbf{c}_k)$ for $i = 1, \dots, k-1$. Write also

$$A = \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{pmatrix}$$

and

$$B = \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_{k-1} \\ \mathbf{c}_k \end{pmatrix}.$$

Then we have $\det(AA^\dagger) = \det(BB^\dagger)$.

Proof: If $k > n$ then $\det(AA^\dagger) = 0 = \det(BB^\dagger)$. If $k = n$ then $\det(A)$ is

$$\begin{vmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{vmatrix} = \begin{vmatrix} \mathbf{e}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{vmatrix} = \begin{vmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{vmatrix} = \dots = \begin{vmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_{k-1} \\ \mathbf{c}_k \end{vmatrix}$$

i.e. $\det(B)$ and hence $\det(AA^\dagger) = \det(BB^\dagger)$.

Assume $k < n$. Let $\mathbf{v}_1, \dots, \mathbf{v}_{n-k} \in \mathbf{C}^n$ be such that $\mathbf{v}_1 \in L(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{0\}$, $\mathbf{v}_2 \in L(\mathbf{v}_1, \mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{0\}$, ..., $\mathbf{v}_{n-k} \in L(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{n-k-1}, \mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{0\}$. Now (as in the case $n = k$) we have

$$\det \begin{pmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \\ \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{n-k} \end{pmatrix} = \det \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_{k-1} \\ \mathbf{c}_k \\ \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{n-k} \end{pmatrix}$$

and hence

$$\begin{vmatrix} \mathbf{c}_1 \mathbf{c}_1^* & \dots & \mathbf{c}_1 \mathbf{c}_k^* & \mathbf{c}_1 \mathbf{v}_1^* & \dots & \mathbf{c}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{c}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & \mathbf{c}_k \mathbf{v}_1^* & \dots & \mathbf{c}_k \mathbf{v}_{n-k}^* \\ \mathbf{v}_1 \mathbf{c}_1^* & \dots & \mathbf{v}_1 \mathbf{c}_k^* & \mathbf{v}_1 \mathbf{v}_1^* & \dots & \mathbf{v}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{v}_{n-k} \mathbf{c}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{c}_k^* & \mathbf{v}_{n-k} \mathbf{v}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

is equal than

$$\begin{vmatrix} \mathbf{e}_1 \mathbf{e}_1^* & \dots & \mathbf{e}_1 \mathbf{c}_k^* & \mathbf{e}_1 \mathbf{v}_1^* & \dots & \mathbf{e}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{e}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & \mathbf{c}_k \mathbf{v}_1^* & \dots & \mathbf{c}_k \mathbf{v}_{n-k}^* \\ \mathbf{v}_1 \mathbf{e}_1^* & \dots & \mathbf{v}_1 \mathbf{c}_k^* & \mathbf{v}_1 \mathbf{v}_1^* & \dots & \mathbf{v}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{v}_{n-k} \mathbf{e}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{c}_k^* & \mathbf{v}_{n-k} \mathbf{v}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}.$$

And since the way we chose $\mathbf{v}_1, \dots, \mathbf{v}_{n-k}$ this means that

$$\begin{vmatrix} \mathbf{c}_1 \mathbf{c}_1^* & \dots & \mathbf{c}_1 \mathbf{c}_k^* & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{c}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & 0 & \dots & 0 \\ 0 & \dots & 0 & \mathbf{v}_1 \mathbf{v}_1^* & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

is equal than

$$\begin{vmatrix} \mathbf{e}_1 \mathbf{e}_1^* & \dots & \mathbf{e}_1 \mathbf{c}_k^* & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{e}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & 0 & \dots & 0 \\ 0 & \dots & 0 & \mathbf{v}_1 \mathbf{v}_1^* & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

because if we write $\mathbf{e}_i = \mathbf{c}_i - \mathbf{x}_i$ where $\mathbf{x}_i \in L(\mathbf{c}_{i+1}, \dots, \mathbf{c}_k)$ then $\mathbf{v}_j \mathbf{e}_i^* = \mathbf{v}_j (\mathbf{c}_i - \mathbf{x}_i)^* = \mathbf{v}_j \mathbf{c}_i^* - \mathbf{v}_j \mathbf{x}_i^* = 0 - 0 = 0$ for all $i = 1, \dots, n-1$ and $j = 1, \dots, n-k$. This gives that

$$|\mathbf{v}_1|^2 \dots |\mathbf{v}_{n-k}|^2 \det(AA^\dagger) = |\mathbf{v}_1|^2 \dots |\mathbf{v}_{n-k}|^2 \det(BB^\dagger)$$

and hence $\det(AA^\dagger) = \det(BB^\dagger)$. ■

Lemma 2.2: Let $V = \mathbf{R}^n$ be an n -dimensional vector space, N a given positive integer, and let $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n \in V$ be a basis for V . Let also U be a k -dimensional subspace of V and $\pi : V \rightarrow U$ an orthogonal projection into U . We can choose a basis $\{\pi(\mathbf{c}_{j_1}), \pi(\mathbf{c}_{j_2}), \dots, \pi(\mathbf{c}_{j_k})\}$ for U such that if $\mathbf{v} = a_1 \mathbf{c}_1 + a_2 \mathbf{c}_2 + \dots + a_n \mathbf{c}_n$ with $|a_i| \leq N$ for all i then $\pi(\mathbf{v}) = b_1 \pi(\mathbf{c}_{j_1}) + b_2 \pi(\mathbf{c}_{j_2}) + \dots + b_k \pi(\mathbf{c}_{j_k})$ with $|b_i| \leq n^2 N$ for all i .

Proof: Since $\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n\}$ is a basis for V we can choose a basis for U from the set $\{\pi(\mathbf{c}_1), \pi(\mathbf{c}_2), \dots, \pi(\mathbf{c}_n)\}$. Without loss of generality we may assume that $\pi(\mathbf{c}_1), \pi(\mathbf{c}_2), \dots, \pi(\mathbf{c}_k)$ are linearly independent. We say that they form a basis K_1 .

Let $\pi(\mathbf{c}_{k+1}) = d_1 \pi(\mathbf{c}_1) + d_2 \pi(\mathbf{c}_2) + \dots + d_k \pi(\mathbf{c}_k)$ for some $d_1, d_2, \dots, d_k \in \mathbf{R}$.

If $|d_i| \leq 1$ for all $i = 1, 2, \dots, k$ then let $K_2 = K_1$.

Otherwise let $|d_j| > 1$ be a maximal coefficient. Now $\pi(\mathbf{c}_j) = \frac{-d_1}{d_j} \pi(\mathbf{c}_1) + \frac{-d_2}{d_j} \pi(\mathbf{c}_2) + \dots + \frac{-d_{j-1}}{d_j} \pi(\mathbf{c}_{j-1}) + \frac{d_{k+1}}{d_j} \pi(\mathbf{c}_{k+1}) + \frac{-d_{j+1}}{d_j} \pi(\mathbf{c}_{j+1}) + \dots + \frac{-d_k}{d_j} \pi(\mathbf{c}_k)$ and the absolute values of coefficients on the right hand side are smaller or equal than one. In this case let $K_2 = (K_1 \setminus \pi(\mathbf{c}_j)) \cup \{\pi(\mathbf{c}_{k+1})\}$. It is clear that K_2 is a basis for U .

Now similarly form a new basis K_{i+1} using basis K_i for all $i = 1, 2, \dots, n-k$ and write $K = K_{n-k+1} = \{\pi(\mathbf{c}_{j_1}), \pi(\mathbf{c}_{j_2}), \dots, \pi(\mathbf{c}_{j_k})\}$.

Now $\pi(\mathbf{c}_l) = d_{l,1} \pi(\mathbf{c}_{j_1}) + d_{l,2} \pi(\mathbf{c}_{j_2}) + \dots + d_{l,k} \pi(\mathbf{c}_{j_k})$ where $|d_{l,i}| \leq n$ for all l and i because every time when we took some $\pi(\mathbf{c}_h)$ off from the basis it then had a such representation in the new basis that all the coordinates were absolutely smaller or equal than zero. Repeating this procedure at most $n-k \leq n$ times and using triangle inequality gives then the property. Hence if $\mathbf{v} = a_1 \mathbf{c}_1 + a_2 \mathbf{c}_2 + \dots + a_n \mathbf{c}_n$ with $|a_i| \leq N$ then $\pi(\mathbf{v}) = b_1 \pi(\mathbf{c}_{j_1}) + b_2 \pi(\mathbf{c}_{j_2}) + \dots + b_k \pi(\mathbf{c}_{j_k})$ with $|b_i| \leq n^2 N$ for all i . ■

Theorem 2.3: For a MIMO-MAC lattice code $(\mathbf{L}_1(N_1), \mathbf{L}_2(N_2), \dots, \mathbf{L}_U(N_U))$ of U users, each transmitting with n transmission antennas, having a code of length $k \geq Un$, and each users lattice is of full rank $r = 2kn$ we have a constant K such that

$$\mathfrak{D}(N_1, \dots, N_U) \leq K \prod_{l=1}^{U-1} N_l^{-\frac{2n^2(U-l)}{k-n(U-l)}}$$

and especially

$$\mathfrak{D}(N) \leq \frac{K}{N^\alpha}$$

where $\alpha = \sum_{l=1}^{U-1} \frac{2n^2(U-l)}{k-n(U-l)}$. Especially if $k = Un$ we have

$$\mathfrak{D}(N_1, \dots, N_U) \leq K \prod_{l=1}^{U-1} N_l^{-\frac{2n(U-l)}{l}}$$

and

$$\mathfrak{D}(N) \leq \frac{K}{N^\beta}$$

where $\beta = \sum_{l=1}^{U-1} \frac{2n(U-l)}{l}$.

Proof: Let us use the notation $C_l = (\mathbf{c}_{l,1}^\top, \dots, \mathbf{c}_{l,n}^\top)^\top$ for $l = 1, \dots, U$.

Let us first fix some small $C_U \in \mathbf{L}_U(N_U)$. Now $|C_U| = \mathcal{O}(1)$. Then write $W_U = \{(\mathbf{x}_1^\top, \dots, \mathbf{x}_n^\top)^\top | \mathbf{x}_i \in L(\mathbf{c}_{U,1}, \dots, \mathbf{c}_{U,n})\}$. Then let $V_U = W_U^\perp$ be its orthogonal complement and $\pi_U : \mathcal{M}_{n \times k}(\mathbf{C}) \rightarrow V_U$ an orthogonal projection.

A subspace V_U has $\dim_{\mathbf{R}}(V_U) = 2nk - \dim_{\mathbf{R}}(W_U) = 2nk - 2n^2 = 2n(k-n)$ so the image $\pi_U(\mathbf{L}_{U-1}(N_{U-1}))$ falls into a $2n(n-k)$ -dimensional hypercube with side length smaller or equal than $(2nk)^2 N_{U-1} = \mathcal{O}(N_{U-1})$ by lemma 2.2 with coordinates having restricted length since projection can only shrink. We also have $|\mathbf{L}_{U-1}(N_{U-1})| = \theta(N_{U-1}^{2nk})$ so using the linearity of π_U and pigeon hole principle we have some $C_{U-1} \in \mathbf{L}_{U-1}(N_{U-1})$ such that

$$\pi_U(C_{U-1}) = \mathcal{O}\left(\sqrt[2n(k-n)]{\frac{N_{U-1}^{2n(k-n)}}{N_{U-1}^{2nk}}} = \mathcal{O}(N_{U-1}^{-\frac{n}{k-n}}).\right.$$

Now similarly build $V_{U-l} = W_{U-l}^\perp$ for $l = 0, \dots, U-2$ by setting $W_{U-l} = \{(\mathbf{x}_1^\top, \dots, \mathbf{x}_n^\top)^\top | \mathbf{x}_i \in L(\mathbf{c}_{U,1}, \dots, \mathbf{c}_{U,n}, \mathbf{c}_{U-1,1}, \dots, \mathbf{c}_{U-1,n}, \dots, \mathbf{c}_{U-l,1}, \dots, \mathbf{c}_{U-l,n})\}$. This gives $\dim_{\mathbf{R}}(V_{U-l}) = 2nk - \dim_{\mathbf{R}}(W_{U-l}) = 2nk - 2n^2(l+1) = 2n(k-nl-n)$. And again we find C_{U-l-1} such that

$$\pi_{U-l}(C_{U-l-1}) = \mathcal{O}\left(\sqrt[2n(k-nl-n)]{\frac{N_{U-l-1}^{2n(k-nl-n)}}{N_{U-l-1}^{2nk}}} = \mathcal{O}(N_{U-l-1}^{-\frac{nl+n}{k-nl-n}}).\right.$$

Lemma 2.1 gives that if $A = (C_1^\top, \dots, C_U^\top)^\top$ and $B = (\pi_2(C_1)^\top, \dots, \pi_U(C_{U-1})^\top, C_U^\top)^\top$ then $\det(AA^\dagger) = \det(BB^\dagger)$ that is of size

$$\mathcal{O}\left(\left(\prod_{l=0}^{U-2} N_{U-l-1}^{-\frac{nl+n}{k-nl-n}}\right)^{2n}\right) = \mathcal{O}\left(\prod_{l=1}^{U-1} N_l^{-\frac{2n^2(U-l)}{k-n(U-l)}}\right).$$

■

REFERENCES

- [1] H.-F. Lu, J. Lahtonen, R. Vehkalahti, and C. Hollanti: *Remarks on the criteria of constructing MAC-DMT optimal codes* presented at the IEEE Inf. Theory Workshop, Cairo, Egypt, 2010.
- [2] J. Lahtonen, R. Vehkalahti, H.-F. Lu, C. Hollanti, and E. Viterbo: *On the Decay of the Determinants of Multiuser MIMO Lattice Codes* presented at the IEEE Inf. Theory Workshop, Cairo, Egypt, Jan. 2010.